REMARKS

Upon entry of the foregoing Amendment, claims 1-35 are pending in the application. Claims 1, 10-11, 16, and 23-24 have been amended. No claims have been cancelled. Claims 32-35 have been newly added. Applicants believe that this Amendment does not add new matter. In view of the foregoing Amendment and the following Remarks, allowance of all the pending claims is requested.

REJECTION UNDER 35 U.S.C. § 103

A. CLAIMS 1-8, 10, 12-14, 16-21, 23, 25-28, AND 30-31

The Examiner has rejected claims 1-8, 10, 12-14, 16-21, 23, 25-28, and 30-31 under 35 U.S.C. § 103 as allegedly being unpatentable over U.S. Patent No. 6,772,345 to Shetty ("Shetty") in view of "An Adaptive Security Model for Mobile Agents in Wireless Networks" to Alampalayam et al. ("Alampalayam"). This rejection is improper and should be withdrawn for at least the reason that the references relied upon, either alone or in combination, fail to disclose, teach, or suggest each and every feature of the claimed invention.

More particularly, neither Shetty nor Alampalayam, either alone or in combination, disclose, teach, or suggest at least the features of "creating an attack profile that includes information based on the detected attack, wherein the attack profile includes information related to the monitored packets that include information associated with the attack signature," and "blocking one or more of the monitored packets that include information associated with the attack profile from being transmitted to the target system," as recited in independent claim 1, for example.

Shetty generally relates to a system "for malware scanning of data that is being transferred or downloaded to a computer system" (Abstract). In particular, Shetty describes protocol filters that "scan the traffic data stream for malwares" and "filter[] the malware out of the data stream" when detected (col. 3, lines 13-20). However, Shetty does not disclose, teach, or suggest the protocol filter "creating an attack profile that includes information based on the detected attack," and "blocking one or more of the monitored packets that include information

associated with the attack profile." Rather, Shetty indicates that when a protocol filter detects malware, the protocol filter filters the malware out of the stream and "then forwards the scanned data to workstation computer applications" (col. 4, lines 25-31). Thus, for at least the reason that Shetty fails to disclose, teach, or suggest using information related to the detection of malware to create an attack profile, and then using such information to determine what data should be blocked from transmission to the target device, Shetty fails to disclose, teach, or suggest at least the foregoing features recited in independent claim 1.

In addition, although Alampalayam generally relates to "a security framework that will detect automatically various attacks and then take appropriate measures to deal with the attack," Alampalayam does not disclose, teach, or suggest such "appropriate measures" as including the creation of an "attack profile [that] includes information related to the monitored packets that include information associated with the attack signature." While Alampalayam generally discusses the use of "adaptive security and holistic security," the security mechanism is specifically characterized as "identifying . . . critical system parameters that are affected by various types of attacks" (Section 2.1). As such, Alampalayam states that "we could measure the relative change in parameter values and detect the type of attack," whereby the security model "uses measured vulnerability metrics and fuzzy logic to evaluate vulnerability" (Sections 2.1-2.2). However, Alampalayam does not disclose, teach, or suggest the security model, or any other feature described therein, as "creating an attack profile" that specifically "includes information related to the monitored packets that include information associated with the attack signature." Instead, the system in Alampalayam specifically focuses on security for a "wireless ad hoc network," where "different devices can interoperate with heterogeneous networks" (Section 1.2). As such, Alampalayam only monitors parameters associated with the end-user device, not packets themselves, to determine whether the device "parameters change rapidly in a given time frame" (Section 2.2). For at least this reason, Alampalayam fails to disclose, teach, or suggest at least the foregoing features recited in independent claim 1.

Accordingly, for at least the foregoing reasons, Shetty and Alampalayam, either alone or in combination, fail to disclose, teach, or suggest each and every feature of independent claim 1. The rejection is therefore improper and should be withdrawn.

Independent claims 10, 16, and 23 include features similar to those set forth in independent claim 1. Dependent claims 2-8, 12-14, 17-21, 25-28, and 30-31 depend from and add features to one of independent claims 1, 10, 16, and 23. Thus, the rejection of these claims is likewise improper and should be withdrawn for at least the same reasons.

B. CLAIMS 9, 11, 15, 22, 24, AND 29

The Examiner has rejected claims 9, 11, 15, 22, 24, and 29 under 35 U.S.C. § 103 as allegedly being unpatentable over Shetty in view of Alampalayam and further in view of U.S. Patent Application Pub. No. 2002/0166063 to Lachman, III et al. ("Lachman"). This rejection is improper and should be withdrawn for at least the reason that the references relied upon, either alone or in combination, fail to disclose, teach, or suggest each and every feature of the claimed invention.

More particularly, for at least the reasons discussed above, Shetty and Alampalayam, either alone or in combination, do not disclose, teach, or suggest at least the features of "creating an attack profile that includes information based on the detected attack, wherein the attack profile includes information related to the monitored packets that include information associated with the attack signature," and "blocking one or more of the monitored packets that include information associated with the attack profile from being transmitted to the target system," as recited in independent claim 1, for example. Lachman fails to cure at least this deficiency of Shetty and Alampalayam.

Accordingly, for at least the foregoing reasons, Shetty, Alampalayam, and Lachman, either alone or in combination, fail to disclose, teach, or suggest each and every feature of independent claim 1. Independent claims 10, 16, and 23 include features similar to those set forth in independent claim 1. Dependent claims 9, 11, 15, 22, 24, and 29 depend from and add features to one of independent claims 1, 10, 16, and 23. Thus, the rejection of these claims is improper and should be withdrawn for at least the foregoing reasons.

CONCLUSION

Having addressed each of the foregoing rejections, it is respectfully submitted that a full and complete response has been made to the outstanding Office Action. As such, the application is in condition for allowance. Notice to that effect is respectfully requested.

If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Date: **June 24, 2008**

Respectfully submitted,

By: _____

Syed Jafar Ali
Registration No. 58,780

PILLSBURY WINTHROP SHAW PITTMAN LLP
P.O. Box 10500
McLean, Virginia 22102
Main: 703-770-7900
Direct: 703-770-7540
Fax: 703-770-7901